[Billing Code: 6750-01-S]

FEDERAL TRADE COMMISSION

16 CFR Part 314

Public Workshop Examining Information Security for Financial Institutions and Information Related to Changes to the Safeguards Rule

AGENCY: Federal Trade Commission.

ACTION: Public workshop and request for public comment.

SUMMARY: The Federal Trade Commission ("FTC" or "Commission") is holding a public workshop relating to its April 4, 2019, Notice of Proposed Rulemaking ("NPRM") announcing proposed changes to the Commission's Safeguards Rule. The workshop will explore information concerning the cost of information security for financial institutions, the availability of information security services for smaller financial institutions, and other issues raised in comments received in response to the NPRM.

DATES: The public workshop will be held on May 13, 2020, from 9:00 a.m. until 4:30 p.m., at the Constitution Center Conference Center, located at 400 7th Street SW, Washington, DC. Requests to participate as a panelist must be received by March 13, 2020. Any written comments related to agenda topics or the issues discussed by the panelists at the workshop must be received by June 12, 2020.

ADDRESSES: Interested parties may file a comment or a request to participate as a panelist online or on paper, by following the instructions in the Filing Comments and Requests to Participate as a Panelist part of the **SUPPLEMENTARY INFORMATION** section below. Write "Safeguards Rule, 16 CFR part 314, Project No. P145407," on your comment and file your comment online at *https://www.regulations.gov* by following the

instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex B), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex B), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: David Lincicum (202-326-2773), Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION:

I. Introduction

In 1999,[1] Congress enacted the Gramm Leach Bliley Act ("GLB" or "GLBA"). The GLBA provides a framework for regulating the privacy and data security practices of a broad range of financial institutions. Among other things, the GLBA requires financial institutions to implement security safeguards for customer information. Pursuant to the GLBA, the Commission promulgated the Safeguards Rule in 2002. The Safeguards Rule became effective on May 23, 2003.

The Safeguards Rule requires a financial institution to develop, implement, and maintain a comprehensive information security program that consists of the administrative, technical, and physical safeguards the financial institution uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.[2] The information security program must be written in one or more

[1] Public Law 106-102, 113 Stat. 1338 (1999).
[2] 16 CFR 314.2(c).

readily accessible parts.[3] The safeguards set forth in the program must be appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of any customer information at issue.[4] The safeguards must also be reasonably designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[5]

In order to develop, implement, and maintain its information security program, a financial institution must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, including in the areas of: (1) employee training and management; (2) information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and (3) detecting, preventing, and responding to attacks, intrusions, or other systems failures.[6] The financial institution must then design and implement safeguards to control the risks identified through the risk assessment, and must regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.[7] The financial institution is also required to evaluate and adjust its information security program in light of the results of this testing and monitoring, as well as any material changes in its operations or business arrangements, or any other circumstances that it knows or has reason to know may have a

[3] 16 CFR 314.3(a).
[4] 16 CFR 314.3(a), (b).
[5] 16 CFR 314.3(a), (b).
[6] 16 CFR 314.4(b).
[7] 16 CFR 314.4(c).

material impact on its information security program.[8] The financial institution must also designate an employee or employees to coordinate the information security program.[9]

Finally, the Safeguards Rule requires financial institutions to take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information and require those service providers by contract to implement and maintain such safeguards.[10]

On August 29, 2016, the Commission solicited comments on the Safeguards Rule as part of its periodic review of its rules and guides.[11] The Commission sought comment on a number of general issues, including the economic impact and benefits of the Rule; possible conflicts between the Rule and state, local, or other federal laws or regulations; and the effect on the Rule of any technological, economic, or other industry changes. The Commission received 28 comments from individuals and entities representing a wide range of viewpoints.[12] Most commenters agreed that there is a continuing need for the Rule and that it benefits consumers and competition.[13]

After reviewing the comments, the Commission published a Notice of Proposed Rulemaking ("NPRM") proposing to amend the Rule to include more detailed requirements for the development and establishment of the information security program required under the Rule, including requirements for encrypting financial information, the

---

[8] 16 CFR 314.4(e).
[9] 16 CFR 314.4(a).
[10] 16 CFR 314.4(d).
[11] Safeguards Rule, Request for Comment, 81 FR 61632 (Sept. 7, 2016).
[12] The comments are posted at: https://www.ftc.gov/policy/public-comments/initiative-674. The Commission has assigned each comment a number appearing after the name of the commenter and the date of submission. This notice cites comments using the last name of the individual submitter or the name of the organization, followed by the number assigned by the Commission.
[13] *See, e.g.*, Mortgage Bankers Association (Comment #39); National Automobile Dealers Association (Comment #40); Data & Marketing Association (Comment #38); Electronic Transactions Association (Comment #24); State Privacy & Security Coalition (Comment #26).

use of multifactor authentication, a written incident response plan, and the creation of periodic reports for the financial institution's board of directors.[14] In addition, the Commission proposed amendments to the definition of "financial institution" and the addition of examples previously contained in the Privacy Rule to clarify the Safeguards Rule.[15] The Commission sought public comment on these proposed amendments as well as requesting information about the cost, benefits and options for information security for financial institutions, particularly smaller institutions. The Commission received 48 comments.[16] Thirteen comments from consumer groups, individuals, academic institutions, and government groups generally supported the addition of more detailed requirements as proposed. Twenty-four comments from industry groups and individuals generally opposed the addition, on the grounds that they would impose unwarranted costs on financial institutions.

II. Issues for Discussion at the Workshop

As part of the Safeguards Rule rulemaking, the FTC has decided to seek additional information about the costs and benefits of the proposed rule changes and the ability of financial institutions to comply with them. The workshop will seek information, empirical data, and testimony from security professionals who have worked with financial services companies, and will cover such topics as:

1) Price models for specific elements of information security programs;

2) Industry standards for security in various industries;

3) How risks of cybersecurity events change based on the size of the financial institutions;

---

[14] 84 FR 13158 (April 4, 2019).
[15] *Id.*
[16] The comments are posted at https://www.regulations.gov/document?D=FTC-2019-0019-0011.

4) Availability of third party information security services aimed at different sized institutions;

5) Different methods of achieving continuous monitoring of information security systems;

6) Costs and optimal frequency of penetration and vulnerability testing and the factors that affect that determination;

7) Best uses for security logs and audit trails;

8) The advantages and disadvantages of having a single person responsible for the information security program;

9) How different corporate governance structures can affect performance of information security programs;

10) Costs of encryption and multifactor authentication, and possible alternatives to these technologies

11) Whether SMS is an appropriate factor for multifactor authentication;

12) The optimal balance between documentation and implementation of security measures.

A more detailed agenda will be published at a later date, in advance of the scheduled workshop.

III. Public Participation Information

A. Workshop Attendance

The workshop is free and open to the public, and will be held at the Constitution Center, 400 7th Street SW, Washington, DC. It will be webcast live on the FTC's website. For admittance to the Constitution Center, all attendees must show valid

government-issued photo identification, such as a driver's license. Please arrive early enough to allow adequate time for this process.

This event may be photographed, videotaped, webcast, or otherwise recorded. By participating in this event, you are agreeing that your image—and anything you say or submit—may be posted indefinitely at www.ftc.gov or on one of the Commission's publicly available social media sites.

B. Requests to Participate as a Panelist

The workshop will be organized into panels, which will address the designated topics. Panelists will be selected by FTC staff. Other attendees will have an opportunity to comment and ask questions. The Commission will place a transcript of the proceeding on the public record. Requests to participate as a panelist must be received on or before March 13, 2020, as explained Section IV below. Persons selected as panelists will be notified on or before March 27, 2020. Disclosing funding sources promotes transparency, ensures objectivity, and maintains the public's trust. If chosen, prospective panelists will be required to disclose the source of any support they received in connection with participation at the workshop. This information will be included in the published panelist bios as part of the workshop record.

C. Electronic and Paper Comments.

The submission of comments is not required for participation in the workshop. If a person wishes to submit paper or electronic comments related to the agenda topics or the issues discussed by the panelists at the workshop, such comments should be filed as prescribed in Section IV, and must be received on or before June 12, 2020.

IV. Filing Comments and Requests to Participate as a Panelist

You can file a comment, or request to participate as a panelist, online or on paper. For the Commission to consider your comment, we must receive it on or before June 12, 2020. For the Commission to consider your request to participate as a panelist, we must receive it by March 13, 2020. Write "Safeguards Rule, 16 CFR 314, Comment, Project No. P145407" and your comment and "Safeguards Rule, 16 CFR 314, Request to Participate, Project No. P145407" on your request to participate. Your comment—including your name and your state—will be placed on the public record of this proceeding, including to the extent practicable, on the publicly available website, *https://www.regulations.gov*.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online, or to send them to the Commission by courier or overnight service. To make sure that the Commission considers your online comment, you must file it at *https://www.regulations.gov*.

Because your comment will be placed on a publicly accessible website, *https://www.regulations.gov*, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number, financial account number, or credit or debit card number. You are also solely responsible for making sure your comment does not include any sensitive health information, such as medical records

or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential"—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)— including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comments to be withheld from the public record.[17] Your comment will be kept confidential only if the FTC General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website, we cannot redact or remove your comment from the FTC website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Requests to participate as a panelist at the workshop should be submitted electronically to *safeguardsworkshop2020@ftc.gov*, or, if mailed, should be submitted in the manner detailed below. Parties are asked to include in their requests a brief statement setting forth their expertise in or knowledge of the issues on which the workshop will focus as well as their contact information, including a telephone number and email address (if available), to enable the FTC to notify them if they are selected.

[17] *See* 16 CFR 4.9(c).

If you file your comment or request on paper, write "Safeguards Rule, 16 CFR part 314, Comment, Project No. P145407" on your comment and on the envelope and "Safeguards Rule, 16 CFR part 314, Request to Participate, Project No. P145407," on your request and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC–5610 (Annex F), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex F). If possible, submit your paper comment or request to the Commission by courier or overnight service.

Visit the Commission website at *https://www.ftc.gov* to read this Notice and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before June 12, 2020. The Commission will consider all timely requests to participate as a panelist in the workshop that it receives by March 13, 2020. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy*.

V. Communications by Outside Parties to Commissioners or Their Advisors

Written communications and summaries or transcripts of oral communications respecting the merits of this proceeding, from any outside party to any Commissioner or Commissioner's advisor, will be placed on the public record.[18]

By direction of the Commission.

April J. Tabor,

Acting Secretary.

[18] *See* 16 CFR 1.26(b)(5).

Concurring Statement of Commissioners Christine S. Wilson and Noah Joshua Phillips

Today the Commission announced a public workshop relating to its April 4, 2019 notice of proposed rulemaking ("NPRM") recommending changes to the Commission's Safeguards Rule. Although we dissented from the issuance of the NPRM, we concur with the decision to hold this workshop. Our dissent from the issuance of the NPRM[1] was based in part on the fact that the FTC lacked an adequate evidentiary basis for the proposed rule's requirements, so we applaud the FTC's willingness to seek additional information, empirical data, and testimony from stakeholders and experts to inform the agency's analysis of potential changes to the Safeguards Rule.

Our dissent expressed several concerns that subsequently were echoed in comments submitted to the FTC during the NPRM process:

- First, we were concerned that the proposed revisions are overly prescriptive. We are wary of trading flexibility for a costly one-size-fits-all approach that would divert company resources away from risk management initiatives specifically tailored to each entity's unique data collection, usage, and storage practices.[2] Our wariness was exacerbated by the fact that the proposal would apply remedies imposed in specific data security enforcement actions—generally outside the context of the Safeguards Rule

[1] Dissenting Statement of Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson, Regulatory Review of Safeguards Rule (Mar. 5, 2019), https://www.ftc.gov/system/files/documents/public_statements/1466705/reg_review_of_safeguards_rule_cmr_phillips_wilson_dissent.pdf.

[2] Comments express similar concerns that the proposal is overly prescriptive and creates costs that may not significantly reduce data security risks or increase consumer benefits. *See* Comments submitted by Office of Advocacy, US Small Business Administration, National Automobile Dealers Association, Mortgage Bankers Association, Global Privacy Alliance, Software Information & Industry Association, and U.S. Chamber of Commerce. NPRM Comments are posted at https://www.regulations.gov/document?D=FTC-2019-0019-0011.

and only to the firms named in those actions—to financial information generally, without a basis to conclude that the Safeguards Rule is not adequate or that covered firms systematically have worse data security than those not covered, such that additional regulation beyond the current Rule would be warranted.

- Second, we were concerned that this new and prescriptive approach would impose significant incremental costs without materially reducing data security risks or significantly increasing consumer benefits.[3] The submission from NADA, by way of example, highlights the incremental costs imposed by the proposed revisions: NADA estimates that it would cost the average car dealership one-time, up-front costs of $293,975, with $276,925 in additional costs each year.[4] These incremental costs will be particularly burdensome for new entrants and smaller companies, which may ultimately hinder competition with larger and better-established rivals.
- Third, we were concerned that the suggested Rule revisions substituted the Commission's judgment for a private firm's governance decisions.[5]
- Fourth, we were concerned that the Rule was premature because the proposed regulations are substantially based on relatively new New York

[3] *See* Comment from the National Independent Automobile Dealers Association (noting the considerable costs imposed on financial institutions from the proposed revisions and the need for the FTC to demonstrate a clear link between its proposal and reductions in data security risks and increases in consumer benefits).
[4] Comment from the National Automobile Dealers Association (NADA), 42.
[5] This sentiment is reflected in the comment from the Software Information & Industry Association.

State Department of Financial Services regulations that have not been market-tested for feasibility and efficacy.[6]

The workshop will enable the FTC to obtain additional information about the costs and benefits of the proposed rule changes and the ability of companies that fall within the Rule's scope to comply with the proposed changes. We continue to encourage stakeholders, including experts in security for financial services companies, to comment and provide evidence for this workshop. We are particularly interested in hearing from those who are knowledgeable about security for small businesses. In light of the significant proposed changes to the Safeguards Rule, and the concerns expressed by many commenters thus far, we view this additional solicitation of input from stakeholders as vital.

[6] Comments express similar concerns that the FTC's proposed regulations rely on untested frameworks and recommend allowing time to assess the impacts of the model legislation. *See* Comments from the Office of Advocacy, US Small Business Administration, CTIA, National Automobile Dealers Association, and Consumer Data Industry Association (CDIA).

Statement of Commissioner Rohit Chopra Joined by Commissioner Rebecca Kelly Slaughter

Summary

- Corporate America's surveillance of our personal data is not just about privacy. Foreign actors are stealing and stockpiling this data, which threatens our national security.
- Companies like Equifax, with their unquenchable thirst for data and their shoddy security practices, are not victims. We must act to curtail the collection, abuse, and misuse of data.
- Rather than "hold our breath and wait" for Congress, the FTC should use the legal authority it has today to protect our citizens, our economy, and our country.

A few weeks ago, U.S. Attorney General William Barr announced criminal indictments against four members of the Chinese People's Liberation Army for conspiring to hack Equifax's computer systems. The Attorney General noted that China has a "voracious appetite for the personal data of Americans" and linked China with several other high-profile hacks of personal data held by large U.S. corporations, including the intrusions into one of America's largest hotel chains, Marriott, and one of America's largest health insurers, Anthem.[1]

The threat posed by China's hacks goes far beyond identity theft. As explained by Attorney General Barr, "these thefts can feed China's development of artificial

[1] William P. Barr, U.S. Attorney General, Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax, Remarks as Prepared for Delivery, (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military

intelligence tools as well as the creation of intelligence targeting packages."[2] Safeguarding personal data is undoubtedly a national security issue.

In spite of these risks, lax security practices continue to expose our data. According to an alert by the Department of Homeland Security, 85 percent of targeted attacks are preventable.[3] For example, it is hard to call Equifax a victim. Their shoddy approach to security was practically an invitation for the Chinese People's Liberation Army to raid Americans' data. Equifax received critical alerts on the need to patch software systems, but failed to do so. Equifax even stored sensitive usernames and passwords in plain text.[4]

The costs of maintaining the status quo approach are significant and mounting. According to industry analysis, the majority of small businesses currently "do not have a cyberattack prevention plan,"[5] yet nearly half of them have experienced at least one breach within the last year.[6] Data breaches can be particularly perilous for small businesses and new entrants, with one survey finding that 66 percent could face temporary or permanent closure if their systems are compromised.[7]

The process of putting into place clear rules requiring corporations to prevent abuse and misuse personal data is long overdue. As the agency responsible for data

---

[2] *Id.*
[3] Press Release, Department of Homeland Security, Alert (TA15-119A) Top 30 Targeted High Risk Vulnerabilities, (Sept. 29, 2016), https://www.us-cert.gov/ncas/alerts/TA15-119A
[4] Fed. Trade Comm'n v. Equifax, Case 1:19-mi-99999-UNA, U.S. District Court for the Northern District of Georgia, Atlanta Division, Complaint for Permanent Injunction and Other Relief at 7-8 (July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf
[5] Craig Lurey, *Cyber Mindset Exposed: Keeper Unveils its 2019 SMB Cyberthreat Study*, KEEPER SECURITY, (July 24, 2019), https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/.
[6] *Hiscox Cyber Readiness Report 2019*, HISCOX LTD., (Apr. 23, 2019), https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/.
[7] Press Release, *VIPRE Announces Launch of VIPRE Endpoint Security - Cloud Edition*, BUSINESS WIRE, (Oct. 2, 2017), https://www.businesswire.com/news/home/20171002005176/en.

protection across most of the economy, the Federal Trade Commission plays a central role.

While the effort to update the Safeguards Rule is a start, its reach will be limited to certain nonbank financial institutions like Equifax, and violations don't even come with any civil penalties. Given the ongoing harms to individuals and our country, we should use every tool in our toolbox to address data security issues. The Commission has urged Congress to act, but I agree with Commissioner Rebecca Kelly Slaughter, who has argued that "we cannot simply hold our breath and wait."[8] There are many ways that we can curtail the collection, misuse, and abuse of personal data, including launching a rulemaking that broadly applies to companies across sectors so there are meaningful sanctions for violators. We have this authority today.

Commissioners Wilson and Phillips argue that we must consider the impact of data security on competition. I agree. Data security must also be top of mind in our competition enforcement work across sectors of the economy. We should be reviewing how mergers can lead to a race to the bottom on data security. We need to rigorously scrutinize data deals. Companies are being bought and sold based on the data they have and the data they can continue to collect. Acquired data is being merged into larger databases and used in ways that people may not have authorized when they signed up for the service or initially provided their information.

[8] Last year, Commissioner Slaughter described how the FTC could use its existing authority to initiate a data protection rulemaking. *See* Rebecca Kelly Slaughter, Commissioner, Fed. Trade Comm'n, Remarks at the Silicon Flatirons Conference at the University of Colorado Law School: The Near Future of U.S. Privacy Law, (September 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf

We need to continue to take a close look at what promises were made in exchange for data access and whether those promises were upheld when the data was sold. We also need to examine how companies are integrating different security systems, whether strong security standards are being maintained, and whether sensitive data is being handled appropriately.

Finally, we need to consider whether there are limits to the amount of data one company can collect and compile, the types of data one company can combine, and the ways in which data can be used and monetized. The scale and scope of data collection that large companies are engaging in has made them – and us – sitting ducks for malicious actors. Since these companies are more fixated on monetizing that data than securing it, their mass surveillance has become a national security threat. Our adversaries know that these large firms have essentially done the dirty work of collecting intelligence on our citizens, and lax security standards make it easy to steal. Ultimately, we need to fix the market structures and incentives that drive firms to harvest and traffic in our private information, so that complacent companies are punished when they don't care about our security needs or expectations.

The extraordinary step of criminal indictments of members of the Chinese People's Liberation Army announced by the Attorney General is yet another wake-up call. Until we take serious steps to curb corporate surveillance, the risks to our citizens and country will only grow as bad actors continue to steal and stockpile our data. The FTC will need to act decisively to protect families, businesses, and our country from these unquantifiable harms.

[FR Doc. 2020-04610 Filed: 3/5/2020 8:45 am; Publication Date: 3/6/2020]